J. Symbolic Computation (1998) **26**, 315–327
Article No. sy980214

Construction of Linear Systems on Hyperelliptic Curves

T. G. BERRY[†]

Depto de Matemáticas Puras y Aplicadas, Universidad Simón Bolívar, Caracas, Venezuela

An algorithm for constructing a basis of a linear system $\mathcal{L}(D)$ on a hyperelliptic curve is described. Algorithms by Cantor and Chebychev for computing in the Jacobian of a hyperelliptic curve are derived as special cases. The final section describes Chebychev's application of his algorithm to elementary integration of elliptic differentials.

1. Introduction

In this paper we assume knowledge of the standard notation and basic results of algebraic curve theory, at the level of Fulton (1969).

Algebraic curve theory centres on the study of linear systems, that is, of the spaces $\mathcal{L}(D)$, with D a divisor on a curve. Thus the central problem of constructive theory is to find effective methods for construction of these spaces. This is solved in general by algorithms coming from the Brill–Noether theory of adjoint curves, or from the "arithmetic" theory of Dedekind–Hensel–Landsberg. (see, e.g., Davenport (1979), Huang and Ierardi (1994), van Hoeij (1994), Volcheck (1994), Haché (1995, 1996), for descriptions of these algorithms oriented to machine implementation). For special types of curves, however, one can expect algorithms, tailored specifically to the type of curve, which are both simpler and faster than the general algorithms. This paper describes such an algorithm for constructing linear systems on hyperelliptic curves. The algorithm has a uniform description for ground fields of all characteristics, including characteristic 2, this latter being interesting in view of possible applications in coding and cryptography. It involves only operations rational over the field of definition of the divisor and contains as special cases the "reduction algorithms" of Cantor and Chebychev which provide distinguished members of linear equivalence classes of divisors of degree 0.

The algorithm is based on a continued fraction expansion. The first to use continued fractions in the hyperelliptic case was Abel. In his study, Abel (1826), found that the integrability of certain hyperelliptic differentials is equivalent to the existence of non-trivial polynomials P, Q solving the polynomial analogue of the Pell equation, $P^2 - Q^2 R = 1$ where R is a given polynomial. The integer Pell equation is well known to be solvable by a continued fraction expansion, so Abel was naturally led to define an analogous continued fraction expansion for $\sqrt{R}$ when R is a polynomial. He found that the existence of a

[†]E-mail: berry@usb.ve

0747–7171/98/090315 + 13 $30.00/0

solution to the polynomial Pell equation is equivalent to the periodicity of the continued fraction expansion, and when the expansion is periodic the whole integer theory carries over to the polynomial case (see Adams and Razar (1980), Berry (1990), Paysan-Le-Roux (1993), for modern versions and extensions of Abel's work). But it was Chebychev, in his paper in (1857) extending Abel's results on elementary integrals to more general hyperelliptic differentials, who showed that continued fractions have applications that go beyond the context of the Pell equation. Chebychev made a quite different use of continued fractions, giving what we call here the Chebychev reduction algorithm; this has nothing to do with periodicity. The algorithm of the present paper is a generalization of this work by Chebychev. While most of Chebychev's work on integration has been rediscovered in recent years, the continued fraction aspect seems to have gone largely unremarked (though Bertrand (1995) describes a related technique). Thus, for intrinsic interest, and as an example of the methods in this paper, the final paragraph describes Chebychev's algorithm.

2. Continued Fractions in Hyperelliptic Function Fields

This section is a summary of results, without proof. Details can be found in Adams and Razar (1980) and Berry (1990).

Let K be an arbitrary field. Let $K((1/X))$ be the field of finite-tailed Laurent series with coefficients in K—we take the uniformizing parameter as $1/X$ for reasons which will shortly become clear. Let $f \in K((1/X))$

$$f = b_k X^k + b_{k-1} X^{k-1} + \cdots b_0 + \frac{b_{-1}}{X} + \cdots.$$

We define

$$\lfloor f \rfloor = b_k X^k + b_{k-1} X^{k-1} + \cdots + b_1 X + b_0$$

and call it the *polynomial part* of f; it is the analogue of the integer part of a real number. Set $a_0 = \lfloor f \rfloor$. If $f = a_0$, stop. Otherwise, define $f_1 \in K((1/X))$ by $f - a_0 = 1/f_1$. By construction f_1 has a non-trivial singular part, so $a_1 = \lfloor f_1 \rfloor \neq 0$. Define f_2 by $f_1 - a_1 = 1/f_2$, and so on. Thus we obtain, as a formal object, the continued fraction expansion

$$f = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}} \tag{2.1}$$

an expression which to save space we shall write as

$$\frac{1}{a_0+}\,\frac{1}{a_1+}\,\frac{1}{a_2+\cdots}.$$

As usual, define the *convergents* p_k, q_k of the continued fraction (2.1) by

$$\frac{p_k}{q_k} = \frac{1}{a_0+}\,\frac{1}{a_1+}\,\frac{1}{\cdots+}\,\frac{1}{a_k}.$$

We note that the expansion (2.1) is finite iff f is a rational function, i.e. lies in the image of the injection $K(X) \to K((1/X))$ given by completion with respect to the valuation at infinity on $K(X)$. When f is a rational function the continued fraction expansion as just defined coincides with the continued fraction expansion obtained from the euclidean algorithm applied to the numerator and denominator of f.

Let v denote the standard discrete valuation on $K((1/X))$. Thus if $h = (\frac{1}{X})^k(b_0 + \frac{b_1}{X} + \cdots) \in K((1/X))$, $k \in \mathbf{Z}$, $b_0 \neq 0$ then $v(h) = k$. In particular, if $\lfloor h \rfloor \neq 0$ then $v(h) = -\deg\lfloor h \rfloor$. The following theorem summarizes the formal properties of continued fraction expansions needed in this paper.

THEOREM 2.1. *Let $f \in K((1/X))$ have the continued fraction expansion (2.1). Then:*

1. *The convergents of the continued fraction expansion are given by the recursion*
   $p_{-1} = 0, p_0 = a_0, q_{-1} = 0, q_0 = 1$
   $p_k = a_k p_{k-1} + p_{k-2}$
   $q_k = a_k q_{k-1} + q_{k-2}, k \geq 1$

2. $v(q_k f - p_k) = \deg q_{k+1}$.

It is worth noting that for $k \geq 1$ one expects that "in general" $\deg a_k = 1$, whence one also expects $\deg q_k = k$ (by Theorem 2.1(1)). The reason is that $\deg a_k$ is the order of the zero obtained by removing the polynomial part of the series f_{k-1}; unless the series is missing the term in $1/X$, which means it is lacunary, this order will be 1. One does not expect an arbitrary Laurent series to be lacunary.

We now specialize to the case of continued fractions derived from Laurent series which are the expansions at infinity of functions in a hyperelliptic function field.

If characteristic $K \neq 2$ then a hyperelliptic curve can be represented as the non-singular model of the plane curve $Y^2 = F(X)$ for some squarefree polynomial $F \in K[X]$. However, in order to treat the case characteristic $K = 2$ on the same footing as other characteristics, we follow an idea in Koblitz (1989). Let C be the non-singular projective model of the plane curve

$$Y^2 + G(X)Y = F(X) \tag{2.2}$$

where $\deg G = g + 1, \deg F = 2g + 2$, and the plane curve (2.2) is non-singular except at infinity (which implies some further conditions on F, G). Then C is a hyperelliptic curve of genus g, and any hyperelliptic curve of genus g can be represented in this way. Let β, γ be the leading coefficients of F, G, respectively. We shall always assume that the equation $T^2 + \gamma T - \beta = 0$ has distinct roots. This condition ensures that C has two distinct points at infinity, which we call ∞^+ and ∞^-. We fix a root α of $T^2 + \gamma T - \beta = 0$ and define ∞^+ to be the point at which the Laurent series of y has leading term αX^{g+1}. (On a curve with equation $Y^2 = F(X)$, if F is monic and $\deg F$ even, it is natural to take as ∞^+ the point corresponding to the branch of y for which $\sqrt{1} = 1$. For general fields, using the model (2.2), there is no such natural choice.)

If a hyperelliptic curve has a K-rational branch point, then this can be taken as at infinity, and in equation (2.2) of the plane model, the degrees are given by $\deg G \leq g$, $\deg F = 2g + 1$. When working with this model we denote the unique point at infinity by ∞.

We identify finite points of C with the corresponding points on the curve (2.2); under this identification, the hyperelliptic involution is $P = (X, Y) \mapsto P^- = (X, -Y - G(X))$. In general, we denote any action of the hyperelliptic involution (on functions, divisors, etc.) by $A \mapsto A^-$.

We may represent $K(C)$, the function field of C, as $K(X, y)$ where the minimal polynomial of y over $K(X)$ is equation (2.2). Then the hyperelliptic involution cor-

responds to the $K(X)$ map $K(C) \to K(C)$ given by $y \mapsto -y - G(X)$. Thus the norm $Nm : K(C) \to K(X)$ on a general element $a + by, a, b \in K(X)$ is given by $Nm(a + by) = a^2 - b^2F - abG$.

Let C be a hyperelliptic curve with two points at infinity, given by equation (2.2). As ∞^+ and ∞^- are unramified, $1/X$ is a uniformizing parameter at each of them, in particular at ∞^+. Any $f \in K(C)$ therefore has at ∞^+ a Laurent expansion in powers of $1/X$, hence also a continued fraction expansion, as described at the beginning of this section. The following theorem describes the basic algorithm for obtaining the expansion. Refinements and generalizations can be found in Berry (1990) and Paysan-Le-Roux (1993).

THEOREM 2.2. *Let $f = (L + y)/M$, $L, M \in K[X], M$ divides $Nm(L + y)$. Then the continued fraction expansion of f at ∞^+ is given by the iteration:*

1. *Initialize*
   $L_0 := L, M_0 := M$;
   $B :=$ *the polynomial of degree $g + 1$ which minimizes* $\deg(B^2 + GB - F)$ *(B is the polynomial part of y)*
2. *Iteration defining a_i. For $i = 0, 1, \ldots$*
   $L_i + B = a_i M_i + r_i$ *(Division Algorithm)*
   $L_{i+1} := B + G - r_i$
   If $i = 0$ then $M_1 := Nm(L_1 + y)/M_0$ else $M_i := M_{i-1} + a_i(r_i - r_{i-1})$.

3. Algorithms for Hyperelliptic Curves

We continue with the notation of Section 2. Unless otherwise stated, C is a hyperelliptic curve with two points at infinity, described by the plane model with equation (2.2).

DEFINITION 3.1.

1. *A* standard finite divisor *on C is an effective divisor whose support consists only of finite points, contains no pair of points twinned in the hyperelliptic involution, and contains branch points to multiplicity at most 1. Explicitly then, an effective divisor $D_0 = \sum n_i P_i$ on C is a standard finite divisor iff all P_i are finite points, $\forall i, j$, $i \neq j$, $P_i \neq P_j^-$ and, if $P_i = P_i^-$ then $n_i = 1$.*
2. *A* standard divisor *is a divisor $D = D_0 + r\infty^-$, where $r \geq 0$ and D_0 is a standard finite divisor.*

PROPOSITION 3.2. *Let D be a standard divisor. If* $\deg D \leq g$ *then $l(D) = 1$. Otherwise,* $l(D) = \deg D + 1 - g$.

The proof is an elementary exercise in the Riemann–Roch theorem on hyperelliptic curves, and is left to the reader.

With $D_0 = \sum n_i P_i$ a standard finite divisor, let $P_i = (x_i, y_i)$. Let $M = \prod (X - x_i)^{n_i}$, and let $L(X)$ be the polynomial of minimal degree such that $L(X) + y$ vanishes to order n_i at P_i^-, the hyperelliptic twin of P_i. Define $f \in K(C)$ by

$$f = \frac{L + y}{M}.$$

Then the divisor of finite poles of f is D_0. We shall refer to f as the *pole function* of D_0. If $D_0 = 0$ then we take the pole function as y. Note that pole functions never lie in $K(X)$. By construction $M|Nm(L+y)$ so the continued fraction expansion of f at ∞^+ is given by Theorem 2.2. Henceforth we refer to this continued fraction expansion simply as *the expansion* of f.

From now on, unless otherwise mentioned, D denotes a standard divisor $D_0 + r\infty^-$ and $f = (L+y)/M$ denotes the pole function of D_0. We set $N = \deg D$, so that $r = N - \deg M$. We shall first give an algorithm for finding $\mathcal{L}(D)$. An algorithm for arbitrary effective divisors is easily derived from this by general theory of hyperelliptic curves. In view of Proposition 3.2 we assume $N \geq g + 1$.

The following simple lemma is useful.

LEMMA 3.3. *Let $p_k, q_k \in k[X]$, $k = 1, \ldots, m$ and suppose the q_k are K-linearly independent. Then the functions $q_k f - p_k \in K(C)$ are K-linearly independent.*

PROOF. The proof is immediate, using $f \notin K(X)$.□

Let v_+, v_- denote the valuations of $K(C)$ at ∞^+ and ∞^-, respectively. We use the following elementary facts: if $q \in K[X]$ then $v_+(q) = v_-(q) = -\deg q$, while $v_+(y) = v_-(y) = -(g+1)$, and, more generally, $v_+(qy) = v_-(qy) = -\deg q - g - 1 \ \forall q \in K[X]$.

LEMMA 3.4. *Let $h = A(X) + B(X)y$ be an arbitrary element in $K(C)$, where $A, B \in K(X)$. If $v_-(h) < v_+(h)$ (strict inequality) then $v_-(h) = -(g+1) + v_-(B)$.*

PROOF. For any discrete valuation v, we have $v(h) = v(A + By) \geq \min(v(A), v(By))$, and strict inequality occurs iff the leading terms of the Laurent series of A and By at the point corresponding to v cancel out, i.e. they are equal and opposite. With our hypotheses

$$v_+(h) > v_-(h) \geq \min(v_-(A), v_-(By)).$$

But $v_-(A) = v_+(A), v_-(By) = v_+(By)$, hence

$$v_+(h) > \min(v_+(A), v_+(By))$$

so that the leading terms of the Laurent series of A and By at ∞^+ are equal and opposite; in particular $v_+(A) = v_+(By)$. Now the Laurent series of A, B are the same at ∞^+ and ∞^-, while the leading term of the series for y at ∞^+ has a coefficient which is definitely distinct from that at ∞^-. Thus there can be no cancellation between the leading terms of the Laurent series of A and By at ∞^-, whence

$$v_-(h) = \min(v_-(A), v_-(By)). \tag{3.1}$$

But $v_-(A) = v_-(By)$ (because as we have just seen this is true with v_+ in place of v_-), and the lemma follows.

For a positive integer i, define $\mathcal{L}_i = \mathcal{L}(D - i\infty^+)$. Note that $\dim \mathcal{L}_i \geq l(D) - i$, by Riemann–Roch. In particular, we have $\dim \mathcal{L}_{N-g} \geq 1$ and $\dim \mathcal{L}_0 = l(D)$. Thus $\mathcal{L}(D)$ has a filtration

$$(0) \subset \mathcal{L}_{N-g} \subseteq \mathcal{L}_{N-g-1} \subseteq \ldots \subseteq \mathcal{L}_j \subseteq \mathcal{L}_{j-1} \subseteq \ldots \subseteq \mathcal{L}_0 = \mathcal{L}(D)$$

which is often useful in practice. Our algorithm will produce a basis of $\mathcal{L}(D)$ compatible with this filtration.

LEMMA 3.5. *Let $p, q \in K[X]$ with $\deg q \leq N-(g+1)$. Then the function $h = qf - p \in \mathcal{L}_i$ iff $v_+(h) \geq i$.*

PROOF. The condition is trivially necessary. To see sufficiency, note first that, because p, q are polynomials, the finite poles of h are no worse than those of f, which by construction are the finite poles of D. Thus $h \in \mathcal{L}(D)$ iff it satisfies the appropriate conditions at infinity, which are $v_+(h) \geq i, v_-(h) \geq -r$. The first of these inequalities is satisfied by hypothesis so it is only necessary to verify the second. If $v_-(h) \geq v_+(h)$ then there is nothing to prove. Thus suppose $v_-(h) < v_+(h)$. Then Lemma 3.4 applies to $h = (qL - pM)/M + qy/M$,and we have $v_-(h) = -(g+1) + v_-(q/M) = -(g+1) - \deg q + \deg M = -(g+1) - \deg q + (N-r) \geq -r$ by hypothesis.

An immediate consequence is

PROPOSITION 3.6. *Let p_k, q_k be convergents of the expansion of f with $\deg q_k \leq N - (g+1)$. Let $i = \deg q_{k+1}$. Then $q_k f - p_k \in \mathcal{L}_i$.*

PROOF. Lemma 3.5 and Proposition 2.1.

Proposition 3.6 already gives an algorithm for generating a basis of $\mathcal{L}(D)$ in the "general" case that $\deg q_k = k, 0 \leq k \leq N-(g+1)$ (cf. the remark following Theorem 2.1). For in this case we find that $\{1, q_k f - p_k : 0 \leq k \leq N-(g+1)\}$ is a set of $N-g+1$ functions in $\mathcal{L}(D)$, and by Theorem 3.2(2) $l(D) = N-g+1$. Thus to see that our functions form a basis of $\mathcal{L}(D)$ it is only necessary to verify that they are linearly independent, and this follows from Lemma 3.3: the polynomials q_k are linearly independent since their degrees are pairwise distinct. However, not all cases are general. A simple example is given by taking C as the genus 2 curve $Y^2 = X^6 + 1$, and $D = D_0$ as the point $(0,1)$ with multiplicity 6. Thus $l(D) = 5$. The pole function of D is $f = (1+y)/X^6$ and its expansion begins

$$f = \frac{1}{X^3 - 1+}\,\frac{1}{2X^3+}\,\frac{1}{2X^3+}\,\frac{1}{2X^3+}\cdots. \tag{3.2}$$

(For an explanation of the periodicity see Berry (1990)), so $q_1 = X^3 - 1$ and already $\deg q_2 > N-(g+1)$. The situation is saved because f has a zero of order 3 at both points at infinity, so that a basis of $\mathcal{L}(D)$ is given by $\{1, f, Xf, X^2 f, q_1 f - p_1\}$. The last entry can be replaced by $X^3 f$, but note that $q_1 f - p_1 \in \mathcal{L}_6$ while $X^3 f$ is not zero at ∞^+.

The main theorem of this section is that a similar method always gives a basis.

THEOREM 3.7. *Let $D = D_0 + r\infty^-$ be a standard divisor of degree N, and let f be the pole function of D_0. Let $(p_k, q_k), k \geq 0$ be the convergents in the expansion of f, and set $f_k = q_k f - p_k$. Let $l \geq 0$ be the index for which $0 \leq \deg q_l \leq N-g-1 < \deg q_{l+1}$. Then the set of functions*

$$\{1\} \cup \{X^\alpha f_l, 0 \leq \alpha \leq N-g-1-\deg q_l\} \cup$$
$$\{X^\beta f_k, 0 \leq \beta \leq \deg q_{k+1} - \deg q_k - 1, 0 \leq k \leq l-1\}$$

form a basis of $\mathcal{L}(D)$. *Moreover the* $X^\alpha f_l \in \mathcal{L}_{j_\alpha}$, $j_\alpha = N - g - \alpha$ *and the* $X^\beta f_k \in \mathcal{L}_{j_\beta}$, $j_\beta = \deg q_{k+1} - \beta$.

PROOF. There are $N - g - 1 = l(D)$ functions of the type described. They are linearly independent by Lemma 3.3 (cf. the remarks following Proposition 3.6), so we have only to prove that they are all in $\mathcal{L}(D)$. It is thus sufficient to prove the final statements of the theorem. Consider the functions $X^\alpha f_l$. The degree of the polynomial which is the coefficient of f in $X^\alpha f_l$ is $\alpha + \deg q_l$, and this by definition of α is $\leq N - (g+1)$. By Proposition 3.6 $f_l \in \mathcal{L}_\lambda$, $\lambda = \deg q_{l+1}$. Then

$$\begin{aligned} v_+(X^\alpha f_l) &= -\alpha + v_+(f_l) \\ &= -\alpha + \deg q_{l+1} \\ &\geq N - g - \alpha \text{ by definition of the index } l \end{aligned}$$

whence by Lemma 3.5 $X^\alpha f_l \in \mathcal{L}_{j_\alpha}$. A similar argument holds for the $X^\beta f_k$.

OBSERVATIONS.

1. Suppose, in the notation of Theorem 3.7, that $r = 0$, i.e. $D = D_0$ is a standard finite divisor. Then, for $0 \leq \deg q_k \leq N - g - 1$ the kth convergents of the expansion of f can be replaced by the kth convergents of the expansion of $L/M \in K(X)$. This can be seen either directly by examining the algorithm of Theorem 2.2, or by imitating the proof of Theorem 3.7 using these convergents. The significance of this observation, apart from a slight speed-up of the algorithm, is that when using the expansion of L/M the algorithm works entirely in the field of definition of $D = D_0$ (which does not necessarily contain the field of definition of the points at infinity). Thus the algorithm in all cases finds $\mathcal{L}(D)$ working entirely over the field of definition of D.
2. Suppose now that C has a single point at infinity. Then the first part of Theorem 3.7, giving the basis of $\mathcal{L}(D)$, still holds for a standard divisor, using the convergents of L/M, as in the previous observation. The proof is precisely analogous to the proof of Theorem 3.7. One uses the rules $v(y) = -2g - 1$ and $v(q(x)) = -2\deg q$ where q is any polynomial, and v denotes the valuation corresponding to the point ∞. Here we define a standard divisor on C as $D_0 + r\infty$ where D_0 is a standard finite divisor, as before, and $r = 0$ or 1. The final part of Theorem 3.7 must be modified using the following proposition. The notation is that of Theorem 3.7.

   PROPOSITION 3.8. *Let* $\mathcal{L}_j$ *denote* $\mathcal{L}(D - j\infty)$. *Then, for* $0 \leq k \leq N - g - 1$, *we have* $f_k \in \mathcal{L}_j$, *where*

$$j = \min(2\deg q_{k+1}, 2(N-r) - 2g - 1 - 2\deg q_k).$$

EXAMPLES.

1. Let C be the genus 2 curve $y^2 = x^6 + 1$, $P = (0,1)$. Let $D_0 = 6P$. Then, as we have already observed, the pole function of D_0 is $f = (y+1)/X^6$, which has expansion (3.2). Thus $\deg q_k = 3k, k \geq 1$. Let $D_r = D_0 + r\infty^-$, $r = 0, 1, \ldots$. Then $l(D_r) = r + 5$, $\deg D_r - (g+1) = r + 3$. Theorem 3.7 gives $\mathcal{L}(D_0) = \{1, X^i f, 0 \leq i \leq 3\}$ as

we have already observed. For $r = 1$ we have $\deg q_1 \leq 4 < \deg q_2$, so the expansion goes to q_1 only, and $\mathcal{L}(D_1) = \{1, X^i f, 0 \leq i \leq 2, X^j f_1, 0 \leq j \leq 1\}$. Similarly $\mathcal{L}(D_2) = \{1, X^i f, 0 \leq i \leq 2, X^j f_1, 0 \leq j \leq 2\}$, and so on. Note we can find $\mathcal{L}(D_0)$ from the (trivial) expansion of $1/X^6$.

2. With C the curve $Y^2 = X^5 + 1$ and $P = (0, 1), D_0 = 5P$, we find $f = (y + 1)/X^5$ which has a zero of order 5 at ∞. The expansion of $1/X^5$ is trivial, and $l(D_0) = \{1, f, Xf, X^2 f\}$, while $l(D_0 + \infty) = \{1, f, Xf, X^2 f, X^3 f\}$.

Finally, we wish to find a basis of $\mathcal{L}(D)$ when D is an arbitrary effective divisor on a hyperelliptic curve C. We can write $D = D_1 + D_2$, where D_1 is a standard divisor and D_2 is "compounded with the hyperelliptic involution", i.e. $D_2 = \sum_{i=1}^{n}(Q_i + Q_i^-)$, where the Q_i are arbitrary points; if C has only one point at infinity, we take $\infty^+ = \infty^- = \infty$. Since $Q + Q^- \equiv \infty^+ + \infty^-$ for any $Q \in C$, we may without loss of generality take $D_2 = n(\infty^+ + \infty^-)$. This simplifies notation. Then

$$\mathcal{L}(D_2) = \{(r(X) + s(X)y) : r, s \in K[X],\ \deg r \leq n, \deg s \leq n - (g + 1)\}.$$

If $D = D_1 + D_2$ with $\deg D_1 \leq g$ then $\mathcal{L}(D) = \mathcal{L}(D_2)$. If $\deg D_1 \geq g + 1$ then find a basis of $\mathcal{L}(D_1)$ using Theorem 3.7. This will consist of functions of the form $qf - p$, $p, q \in K[X]$. Let f_r be the element of this basis for which the polynomial q has maximal degree. Then a basis for $\mathcal{L}(D)$ is given by the basis of $\mathcal{L}(D_1)$, together with the functions $\{X^i, X^i f_r : 1 \leq i \leq n\}$. These assertions follow easily from general theory of hyperelliptic curves.

3.1. REDUCTION ALGORITHMS

For a brief moment, let C denote a general, not necessarily hyperelliptic, curve of genus g, and let D be a divisor of degree 0 on C. Thus $D = D_1 - D_2$ where D_1 and D_2 are effective divisors of the same degree N. If $N \leq g$ then D is said to be *reduced*. If $N > g$ then a reduced divisor D^* which is linearly equivalent to D is called a *reduction* of D, and a function $f \in K(C)$ such that $(f) + D = D^*$ is a *reducing function* for D. Reductions certainly exist: if $N > g$ then there exists an effective divisor D', of degree $N - g$ and $D' \leq D_2$. By Riemann–Roch, there is at least one non-trivial function $f \in \mathcal{L}(D_1 - D')$ and one immediately checks that any such function is a reducing function for D. A *Reduction Algorithm* is an algorithm which produces reducing functions and reductions. Reduction algorithms provide distinguished representatives for divisor classes of degree 0, i.e. of elements of the Jacobian of C. They do not, in general, provide unique representatives unless the reduced divisor satisfies extra conditions.

We now return to the case C a hyperelliptic curve, and describe two variants on the theme of reduction algorithms.

JACOBIAN REDUCTION. The algorithm to be described was given by Cantor (1987), and extended to characteristic 2 by Koblitz (1989).

Let C be a hyperelliptic curve with a single point at infinity, denoted as before by ∞. *Jacobian reduction* is the reduction of an arbitrary divisor of degree 0 to a reduced divisor $D^* - r\infty$, where D^* is a standard finite divisor. Using $P + P^- \equiv 2\infty$ for all points $P \in C$, it is easy to see that any divisor of degree 0 on C is linearly equivalent to a divisor $D - N\infty$, where D is a standard finite divisor (in general with $N > g$), so the key step in Jacobian reduction is reducing divisors of this type. The following theorem produces a reducing function for these divisors in the sense of the first paragraph of this

section, i.e. it reduces the divisor to $D_1 - r\infty$, $r \leq g$, but D_1 may not be a standard finite divisor, because it may contain points paired in the hyperelliptic involution. However, it is easy to deduce a Jacobian reduced divisor from this. For details see Cantor (1987).

THEOREM 3.9. *Let $D = D_0 - N\infty$ where D_0 is a standard finite divisor of degree N. Let the pole function of D_0 be $f = (L + y)/M$ and let (p_k, q_k) be the convergent of the expansion of L/M for which $\deg q_k \leq (N - g - 1)/2 < \deg q_{k+1}$. Then $q_k f - p_k$ is a reducing function for D.*

PROOF. By Proposition 3.8 $q_k f - p_k \in \mathcal{L}(D_0 - (N - g)\infty)$, hence is a reducing function for D, as remarked in the first paragraph of this section.

CHEBYCHEV REDUCTION. Let C now be an arbitrary hyperelliptic curve. There may or may not be ramification at infinity.

THEOREM 3.10. *A divisor of the form $\sum_{i=1}^{N}(P_i - P_i^-)$ is always linearly equivalent to a divisor $\sum_{i=1}^{r}(Q_i - Q_i^-)$ with $r \leq g$.*

PROOF. Let B be an arbitrary branch point of C. Let $D = \sum_{i=1}^{N} P_i - NB$. Then by Jacobian reduction $D \equiv D_1 - rB$ where D_1 is a standard finite divisor of degree $r \leq g$. Then, applying the hyperelliptic involution, $D^- \equiv D_1^- - rB$, and subtracting gives $D - D^- \equiv D_1 - D_1^-$, which is the sought reduction.

We call the type of reduction described by Theorem 3.10 *Chebychev reduction*, as it was introduced in Chebychev (1857). Chebychev reduction occurs naturally (see the next section) and it is interesting to the extent that it can be achieved on curves with two points at infinity without explicitly using Jacobian reduction.

THEOREM 3.11. *Let C be a hyperelliptic curve with two points at infinity, and let D be a standard divisor of degree $N \geq g + 1$. Let $f = (L + y)/M$ be the pole function of the finite part of D. If there exists an index k for which the convergents (p_k, q_k) satisfy*

$$\deg q_k < (N - g - 1)/2 < \deg q_{k+1}$$

with strict inequalities, then the function f_k/f_k^- is a reducing function for $D - D^-$, where $f_k = q_k f - p_k$.

PROOF. For arbitrary $h \in \mathcal{L}(D)$ we may write

$$(h) + D = Z + a\infty^+ + b\infty^- \tag{3.3}$$

where Z is a divisor supported on finite points, $a, b, \geq 0$. Taking degrees on both sides, we have

$$N = \deg Z + a + b. \tag{3.4}$$

Applying the hyperelliptic involution to (3.3) and subtracting gives

$$(h/h^-) + (D - D^-) = Z - Z^- \pm |a - b|(\infty^+ - \infty^-) \tag{3.5}$$

where an appropriate sign is to be chosen for the final term. The right-hand side of (3.5) is a Chebychev reduced divisor provided that $\deg Z + |a - b| \leq g$. Substituting for $\deg Z$

from equation (3.4), we find that the right-hand side of (3.5) is Chebychev reduced, hence h/h^- is a Chebychev reducing function for $D - D^-$, iff

$$N - (a + b) + |a - b| \leq g$$

which comes down to

$$N - g \leq 2\min(a, b). \tag{3.6}$$

Now take $h = f_k = q_k f - p_k$. Then $a = \deg q_{k+1}, b = r + v_-(h)$ where r is the multiplicity of ∞^- in D. If $v_-(h) \geq v_+(h)$ then $\min(a, b) = a = \deg q_{k+1}$ and (3.6) is satisfied if $(N - g)/2 \leq \deg q_{k+1}$, which is equivalent to the right-hand strict inequality of the Theorem. If $v_-(h) < v_+(h)$ then $v_-(h) = \deg M - \deg q_k - (g + 1)$ (cf. Lemma 3.4) so $b = N-(g+1)-\deg q_k$. If $b = \min(a, b)$ then substituting in (3.6) yields $2 \deg q_k \leq N-g-2$ which is equivalent to the left-hand inequality of the theorem.

The index k required by Theorem 3.11 always exists if $N - g - 1$ is odd. Unfortunately, if this number is even, it is more likely than not that the index does not exist. This (non-existence) certainly occurs for $N = g + 1$, and will probably occur for larger N, since in general $\deg q_{k+1} = \deg q_k + 1$. Not all is lost, however. Let D be a standard divisor of degree N where $N - g - 1$ is even. Let B a divisor of odd degree which is a sum of branch points with multiplicity 1. Set $D^* = D + B$. Then D^* is a standard divisor, $\deg D^* - g - 1$ is odd, and $D^* - (D^*)^- = D - D^-$ so we obtain the Chebychev reduction of $D - D^-$ as the reduction of $D^* - (D^*)^-$. By this device it may be possible to achieve Chebychev reduction of D by operations rational over the field of definition of D, even though no branch point is defined over this field. Take for example, over a field K of Char. $\neq 2$ the curve C defined by $Y^2 = F(X)$ where $F \in K[X]$ has even degree, and has no roots in K, but has a factor of odd degree. Then C has no K-rational branch points, but the factor defines a divisor B of odd degree, supported on branch points, and with field of definition K. Thus B can be used to give Chebychev reduction for all divisors on the curve without extension of the field of definition. When there is a rational branch point, this method gives Chebychev reduction directly, without having to transform the branch point off to infinity to use Jacobian reduction. An example is given in the next section.

4. Integration of Elliptic Differentials, after Chebychev

In this section we describe the elegant algorithm of Chebychev (1857) for finding logarithmic integrals on elliptic curves. First we give a rapid summary of the general theory. Details can be found in Davenport (1979).

Let ω be a differential on a curve C, defined over $K = \mathbf{C}$, whose only singularities are simple poles. Then ω is said to be *elementarily integrable* if there are $f_i \in K(C), c_i \in K$ such that $\omega = \sum_{i=1}^{k} c_i df_i/f_i$. We wish to give an algorithm to determine an elementary integral (i.e. the set of c_i, f_i) of ω, if it exists, or to show that it does not exist.

Suppose the poles of ω are at $P_1, \ldots, P_n$ with residues $\rho_1, \ldots, \rho_n$. Suppose $\mu_j, j = 1, \ldots, r$ are a free basis of the $\mathbf{Z}$-module generated by the ρ_i. Then

$$\rho_i = \sum_{j=1}^{r} n_{ij}\mu_j$$

for some $n_{ij} \in \mathbf{Z}$. Define divisors D_j by

$$D_j = \sum_{i=1}^{n} n_{ij} P_i,\ j = 1 \ldots r.$$

A necessary condition for ω to be elementarily integrable is that all D_j be torsion divisors, i.e. that there exist positive integers r_j, and functions $f_j \in K(C)$, $j = 1 \ldots r$, such that $r_j D_j = (f_j)$. If this condition is satisfied then either $\omega = \sum_{j=1}^{r} (\mu_j / r_j) df_j / f_j$ or ω is not elementarily integrable.

Now let C be a hyperelliptic curve of genus g with equation $Y^2 = F(X)$, where F is squarefree. It is easy to reduce the general problem of elementary integrability of differentials with only simple poles on C to the problem with $\omega = R(X)dX/y$, where $R(X) \in K(X)$ has only simple poles. Then the poles of ω occur as pairs of points of C lying over the poles of R, and the residues at P, P^- occur as pairs $\pm\alpha$. It follows that all the divisors D_j defined in the previous paragraph are of the form $\sum(P_i - P_i^-)$, and it is necessary to determine whether these are torsion divisors. We apply Chebychev reduction to reduce the problem to that of determining whether certain divisors $\sum_{i=1}^{r}(Q_i + Q_i^-)$, $r \leq g$, are torsion divisors. But suppose $g = 1$. Then $r = 0$ or 1. If $r = 0$ then $D_j \equiv 0$, so $r_j = 1$. If $r = 1$ then the reduced divisor is just $Q - Q^-$, and by transforming it into $\infty^+ - \infty^-$, the problem is reduced to the one solved by Abel (1826). Thus Chebychev's algorithm uses continued fractions in two different ways, once for the reduction, and once for Abel's solution. Abel's solution comes down to solving the polynomial Pell equation, i.e. to finding $A, B, \in K[X]$ such that $A^2 - B^2 F = 1$, and this is solved by considering the continued fraction expansion of $y = \sqrt{F}$ at ∞^+, a method motivated of course by the classical solution of the Pell equation in $\mathbf{Q}$. But the matter does not end there! To provide a termination condition for Abel's algorithm one must have a bound on the possible torsion, or, what is the same thing, a bound on the degrees of the polynomials solving the Pell equation. When working over a number field, one can use further continued fraction expansions to get this! Namely, if l_1, l_2 are primes of the number field where C has good reduction, which means simply that F remains squarefree when reduced mod l_i, then a torsion bound on C can be obtained from the bounds on the curves $C_i = C \bmod l_i$ (see, e.g., Davenport (1979)). The C_i are curves over finite fields, so all divisors of degree 0 have finite order, and Abel's algorithm on C_i is guaranteed to terminate, giving the torsion of $\infty^+ - \infty^-$. Thus we obtain via continued fraction expansions an efficient algorithm, of great conceptual simplicity, for integration on elliptic curves.

Chebychev did not give the method of reduction mod l_i for obtaining a torsion bound—it depends on concepts developed 50 years later. Instead in two subsequent papers (Chebychev, 1860, 1861), he gave a complicated theorem for the case when everything is defined over $\mathbf{Q}$, which must in some sense be equivalent to the Lutz–Nagel theorem.

EXAMPLE. This is Chebychev's example.

Let C be the curve $Y^2 = X^4 + 4X^3 + 2X^2 + 1$ and let

$$\omega = \frac{(6X^2 + 5X + 7)}{(2X^2 - 1)} \frac{dX}{y}.$$

Then a short calculation shows that ω has poles at points $P_1 = (1/\sqrt{2}, (1+\sqrt{2})/2), P_2 = (-1/\sqrt{2}, (1-\sqrt{2})/2)$ and their hyperelliptic twins. The residues at P_1 and P_2 are $\pm 5/2$. The set D_j consists of a single divisor D_1. If we take $5/2$ as the generator of the $\mathbf{Z}$-module of residues, then $D_1 = D - D^-$ where $D = P_1 + P_2$. As D has degree 2, and $g = 1$ we

fall into the "bad" case of Chebychev reduction. Fortunately there is a rational branch point $R = (-1, 0)$ on C so we take $D^* = D + R$ and reduce $D^* - D^{*-}$. The pole function of D^* is $h = (L + y)/M$ where $L = (X + 1)(1 - 3X)$ and $M = (X + 1)(X^2 - 1/2)$. The degree bounds of Theorem 3.11 show that we should take the zeroth convergent of the expansion of h (or of L/M, as D^* has no point at infinity), i.e. the reducing function is just h/h^-. To find the reduced divisor, we note that, by construction, (cf. the proof of Theorem 3.11) $(h) = -P_1 - P_2 + Q + R$ where $Q - Q^-$ is the reduction of D^*. Thus Q is obtained as the zero of h which is not a zero of y. The zeros of h are found as the zeros of $Nm(L+y) = L^2 - F$, and calculation (or, in the present case, direct observation) yields $Q = (0, -1)$. Transforming $Q - Q^-$ to infinity by $Z = 1/X, Y = T$ (so Q goes to ∞^- with the natural choice of ∞^+ mentioned in Section 2) we find the curve $T^2 = Z^4 + 2Z^2 + 4Z + 1$, and the expansion of the function $t = \sqrt{Z^4 + 2Z^2 + 4Z + 1}$ at ∞^+ is

$$Z^2 + 1 + \frac{1}{Z/2+}\,\frac{1}{2Z - 2+}\,\frac{1}{Z/2+}\,\frac{1}{2(Z^2+1)+}\,\frac{1}{Z/2+}\,\frac{1}{2Z - 2 + \cdots}$$

where the ... indicate periodicity. Thus, (see Abel (1826), Adams and Razar (1980), and Berry (1990)) setting

$$\begin{aligned}\frac{p}{q} &= Z^2 + 1 + \frac{1}{Z/2+}\,\frac{1}{2Z - 2+}\,\frac{1}{Z/2} \\ &= \frac{Z^5 - Z^4 + 3Z^3 + Z^2 + 2}{Z^3 - Z^2 + 2Z}\end{aligned}$$

we have

$$\left(\frac{p - qt}{p + qt}\right) = 10(\infty^+ - \infty^-)$$

where ∞^+, ∞^- refer to points at infinity on the curve in the (Z, T)-plane. Transforming back to the (X, Y)-plane, we find $10(Q - Q^-) = (f)$ where

$$f = \frac{\tilde{p} + \tilde{q}y}{\tilde{p} - \tilde{q}y}$$

and $\tilde{p} = X^5 p(1/X)$ $\tilde{q} = X^3 q(1/X)$. Now

$$\left(\frac{h}{h^-}\right) = -D_1 + (Q - Q^-)$$

whence, putting everything together,

$$10D_1 = 10\left(\frac{h^-}{h}\right) + (f).$$

Set

$$G = \left(\frac{h^-}{h}\right)^{10} f$$

where the bracket does not this time indicate the divisor of the function within! By the general theory of elementary integration summarized at the beginning of this section, either

$$\omega = \frac{5}{-2.10}\,\frac{dG}{G}$$

or ω does not have an elementary integral. In fact, equality holds, as Chebychev verified by hand and the present author by Maple.

This technique in fact can be extended all hyperelliptic curves, as Chebychev hints in the introduction to Chebychev (1865). Details are left for another time.

Acknowledgements

The author thanks the two referees, whose comments have done much to improve both the accuracy and the readability of the paper.

References

Abel, N.H. (1826). Über die Integration der Differential-Formel $\rho dx/\sqrt{R}$ wenn ρ und R ganze Functionen sind. *J. Reine und Angw. Math.*, **1**:185–221.

Adams, W.W., Razar, M.J. (1980). Multiples of points on elliptic curves and continued fractions. *Proc. LMS*, **41**, 481–498.

Berry, T.G. (1990). On periodicity of continued fractions in hyperelliptic function fields. *Arch. Math.*, **55**, 159–226.

Bertrand, L. (1995). Computing a hyperelliptic integral using arithmetic in the Jacobian of the curve *App. Alg. Eng. Comm. Comput.*, **6**, 275–298.

Cantor, D. (1987). Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, **48**, 95–101.

Chebychev, P.L. (1857). Sur l'intégration des différentielles irrationelles qui contiennent une racine carrée d'un polinome du troisième ou du quatrième degré. *Oevres Completes, Vol 1,* Chelsea, New York (undated).

Chebychev, P.L. (1860). Sur l'intégration des différentielles irrationelles. *Oevres Completes, Vol 1*, pp. 511–514, Chelsea, New York (undated).

Chebychev, P.L. (1861). Sur l'integration de la différentielle $\frac{x+A}{\sqrt{x^4+\alpha x^3+\beta x^2+\gamma x+\delta}}dx$. *Oevres Completes, Vol 1*, pp. 515–530. Chelsea, New York (undated).

Chebychev, P.L. (1865). Sur l'intégration des différentielles qui contiennent une racine cubique. *Oevres Completes, Vol 1*, pp. 563–608. Chelsea, New York (undated).

Davenport, J.H. (1979). *On the Integration of Algebraic Functions. (Lecture Notes in Computer Science*, **102**). Springer, Berlin.

Fulton, W. (1969). *Algebraic Curves.* Benjamin, New York.

Haché, G. (1995). Effective construction of algebraic geometry codes. *IEEE Trans. Inf. Theory*, **41**, 1615–1628

Haché, G. (1996). Construction effective des codes géometriques, Thèse, Université Pierre et Marie Curie, Paris VI.

van Hoeij, M. (1994). An algorithm for computing an integral basis in a function field. *J. Symb. Comput.*, **18**, 353–363.

Huang, M.-D. and Ierardi, D. (1994). Efficient algorithms for the Riemann–Roch problem and for addition in the Jacobian of a curve. *J. Symb. Comput.*, **18**, 516–539.

Koblitz, N. (1989). Hyperelliptic cryptosystems. *J. Crypt.*, **1**, 139–150.

Paysan-Le-Roux, R. (1993). Periodicité des fractions continues dans un corps de fonctions hyperelliptiques. *Arch. Math.*, **61**, 46–58w.

Volcheck, E. (1994). Computing in the Jacobian of a plane algebraic curve. In Adleman, L.H., *et al.*, eds, *Algebraic Number Theory, First International Symposium ANTS-1.* Ithaca, NY.

Originally received 14 February 1997
Accepted 27 October 1997